SPECIFICATION AMENDMENTS

Replace the paragraphs at page 4, line 28 to page 7, line 22 with the following paragraphs:

Fig. 1 illustrates~~d~~ a generalized system block diagram 10 of an extremely secure system for keying stored contents to a storage medium in accordance with the principles of the present invention. The extremely secure keying stored content system 10 comprises a host system 12 comprising a host interface 14 coupled to a host microprocessor 16, which is then coupled to other host system hardware generalized for simplicity here as general system 17. Host system 12 stores an extremely secure software application ~~100~~ to be later described in further detail with reference to Figs. 2-4. Extremely secure system 10 also comprises a disk drive unit 20 coupled to host unit 12 via a host-to-drive interface 18. Disk drive unit 20 comprises an interface and storage medium processor system 22, a servo system 24, a read/write system 26, a preamplifier 28, and one or more storage disks 30~~, and a preamplifier 28~~. Preamplifier 28 reads a PSUVI characteristic corresponding to, for example, "the defect list," or any other PSUVI characteristic associated with one or more storage disks 30. The read PSUVI characteristic is then used by host system 12 to encrypt a source content stored on the one or more storage disks 30.

A2

Figs. 2A and 2B illustrate generalized flowcharts of extremely secured method 100 for keying stored contents to the storage medium (Fig. 2A) and for reading and verifying fingerprinted contents of stored information (Fig. 2B) in accordance with the present invention. In general as illustrated by this embodiment, in a first step 104 during a "storing fingerprinted contents" operation 102, a request is sent by host processor 16 to disk drive processor 22 to read a PSUVI characteristic, such as the defect list. During a second step 106, the read defect list is then combined with a specified file content to be secured to generate a fingerprinted content. In a step 146 (Fig. 3), the fingerprinted content can be encrypted first prior to storing. Then in step 108, host processor 16 then commands disk processor 22 to store the fingerprinted content on disk 30. During a "reading and verifying fingerprinted contents" operation 110, in step 112 the host processor 16 commands the disk drive processor 22 to read fingerprinted content. In step

114, host processor 16 separates content and fingerprint. Subsequently, host processor 16 requests fingerprint from disk drive processor 22 in step ~~storage device~~ 116. Then in step 118, host processor 16 compares content and storage device fingerprint. In a last step 120, the host processor 16 decides to use or not to use content based on comparison in step 118.

Fig. 3 illustrates in greater detail a sample method of storing fingerprinted content 102. In this example, host processor 16 would execute steps wherein host processor 16 requests a fingerprint from a storage device 20, such as a defect list from storage device 20, follow by step 106 wherein host processor 16 combines content of a file to be secured with the retrieved fingerprint, and step 108 wherein host processor 16 commands storage device 20 to store fingerprinted content. As illustrated in more detail in Fig. 3, one embodiment to step 104 of requesting a fingerprint comprises:

1. Host 12~~6~~ using open protocol to request secured communication from HDD 20 in step 130;
2. HDD 20 identifies a PSUVI characteristic, such as a defect list in step 132;
3. HDD 20 then generates a decryption key and encryption key in step 134;
4. HDD 20 then returns encryption key to host 12~~6~~ in step 136;
5. Host 12~~6~~ then uses encryption key and switches to encrypted protocol in step 138;
6. Host 12~~6~~ then requests fingerprint PSUVI characteristic 140; and then
7. HDD 20 replies with PSUVI fingerprint in step 142.

As illustrated in more detail in Fig. 3, one embodiment to step 106 of combining content to be secured with the retrieved fingerprint comprises:

1. Host 12~~6~~ creating a hybrid content by combining content and fingerprint in step 144; and
2. Host 12~~6~~ encrypting hybrid content with public key in step 146.

Additionally, step 108 of storing fingerprinted content may comprise host 12~~6~~ commanding HDD 20 to write hybrid content in step 148.

Fig. 4 illustrates in greater detail a generalized method 110 of reading and authenticating a source content method of Fig. 2B. In this example, generalized method 110 of reading and

verifying fingerprinted content comprises a first step 112 of a host processor 16 commanding storage device 20 to read fingerprinted content. For convenience of illustration, we assume processor used in this example is host processor 16. However, it is envisioned that the processor or host referred to and used herein to implement method 110 of reading and verifying source content can be generally a processor in any host system coupled to a storage device 20. Method 110 further comprises step 114 wherein host processor 16 separates file contents to retrieve the fingerprint content. Subsequently, in step 116, host processor 16 requests current storage device 20 to provide fingerprint information. Host processor 16 then compares in step 118 fingerprint separated in step 114 with fingerprint retrieved in step 116 to verify fingerprints, and finally in step 120, host processor 16 then decides whether to use or not to use content based on the comparison step 118.

A2

Fig. 4 further illustrates a sample detailed embodiment of steps described above for method 112 to read and verify fingerprinted contents.

1. Reading the defect list from the HDD 20 (steps 160 and 162).
2. Decrypting the encrypted content. Parsing the vector subparts from the contents (steps 164-170)
3. Reassembling the subparts into a P-list vector (step 172).

More ~~detailed~~ implementation details for steps described in method 110 are also provided ~~also~~ in Fig. 4 and are self-explanatory. Different possible embodiments of methods to verify authenticity of a copied file are envisioned and contemplated. The following described sample methods include using the defect list of a disk:

Replace the paragraph at page 10, lines 4-10 with the following paragraph:

Foregoing described embodiments of the invention are provided as illustrations and descriptions. They are not intended to limit the invention to the precise form described. In particular, it is contemplated that functional implementation of the invention described herein may be implemented equivalently in hardware, software, firmware, and/or other available functional components or building blocks. Other variations and embodiments are possible in

A3

A3 light of the above teachings, and it is thus intended that the scope of the invention not be limited by this Detailed Description, but rather by Claims following.